a

Abstract of the Disclosure

~~Abstract~~

Method and arrangement for the computer-aided interchange of cryptographic keys between a first computer unit and a second computer unit

The invention relates to a method which can be used to declare a session key (K) between a first computer unit (U) and a second computer unit (N) without it being possible for an unauthorized third party to obtain useful information regarding the keys or the identity of the first computer unit (U). This is achieved by embedding the principle of El-Gamal key interchange in the method with additional formation of a digital signature using a hash value whose input variable contains at least variables which can be used to infer the session key unambiguously.